Attachment to Bank Indonesia Circular Number 6/18/DPNP, dated 20 April 2004

Guidelines on Risk Management Application to Bank Services through Internet (Internet Banking)

Directorate of Banking Research and Administration

2004

Table of Contents

		Page
I.	INTRODUCTION	2
II.	PRINCIPLES OF RISK MANAGEMENT APPLICATION - INTERNET BANKING	
	1. Active Supervision of Bank's Board of Commissioners and Board of Directors	3
	2. Security Control	3
	3. Management of Legal Risks and Reputation Risks	4

I. INTRODUCTION

Information technological development has affected the policies and strategies of the banking business world that further motivated innovation and competition in the field of services, particularly payment services through Banks. Innovation of the technologically-based banking services has continued to develop following the needs of the Bank customers. Electronically-based banking transactions, including the Internet, is one of the types of developing the provision of Bank services that provides a new business opportunity that impacts the banking business strategy changes from humans (traditional) to the information technology basis, which is more efficient for the Banks and more practical for the customers.

However, while the Banks have significant benefits from the technological innovation through the internet-based banking transactions, they also face the risks adhering to such activities, among others the risks of the strategy, reputation and operation, including the risks of security and legal, credit, market and liquidity. Basically, internet banking does not cause new risks to arise, which is different from the banking service products through other media. However, we are aware that internet banking increases such risks. Internet banking, particularly, increases the risks of the strategy and operation, including the risks of security, legal and reputation. Therefore, in addition to making use of the new opportunity, the Banks shall identify, measure, monitor and control such risks by means of the principle of prudence.

Basically, the principles applied to the Bank risk management are generally applicable to the internet banking activity. However, such principles shall be adjusted by taking into

account the specific risks adhering to the activity. Based on the matter, the risk management principle of internet banking is divided into three parts that are inseparable and complement each other, namely active control of the Bank's Board of Commissioners and Board of Directors, security control, and management of the legal and reputation risks as follows:

1. Active Control of the Bank's Board of Commissioners and Board of Directors

As the Bank's Board of Commissioners and Board of Directors are responsible for developing the Bank's business strategies and for establishing effective management control, administration of the internet banking activity shall be based on a written policy, which is informative and obvious, established by the Bank's Board of Commissioners and Board of Directors. Effective management control includes, among others, the agreement and restudy of the main aspects of the Bank security control process.

2. Security Control

The security control process requires special attention of the management, due to the increasing security risks caused by the internet banking activity. In connection therewith, the Banks shall examine the customers' identities, the authentication of the transactions, application of the principle of separation of duties, control over the use of the right to access to the system, maintenance of data integrity and confidentiality of important information on internet banking.

3. Management of Legal and Reputation Risks

In order to protect the Banks against the legal and reputation risks, the internet banking services shall be carried out consistently and timely in accordance with the customers' expectations. In order to meet the customers' expectations, the Banks shall have the capacity, business continuity and effective emergency planning. Effective incident response mechanisms are also essential to minimize the risks of operation, legal and reputation arising out of unexpected incidents. In addition, the Banks shall understand and manage the risks arising out of the relationship of the Banks and the third parties in the internet banking administration.

II. PRINCIPLES OF RISK MANAGEMENT APPLICATION – INTERNET BANKING

1. Active Control of the Bank's Board of Commissioners and Board of Directors

a. The Board of Commissioners and the Board of Directors shall control effectively the risks relating to the internet banking activity, including the establishment of accountability, policy and control process to manage the risks.

1) The Board of Commissioners shall approve of the policies relating to the internet banking activity and evaluate the implementation of the internet banking policies submitted by the Board of Directors.

2) The Board of Directors shall restudy the plan to carry out internet banking, which is potential to impact significantly the Bank's strategies and risk profile, including the analysis of costs and benefits of the internet banking plan.

3) The Board of Directors shall ensure that the Bank has, upon entering the internet banking activity, had adequate risk management. In addition, the Board of Directors shall ensure that the officials or employees relating to the internet banking activity are competent in the application and technology that support the Bank's internet banking.

4) The Board of Directors shall monitor periodically the reputation risks adhering to internet banking, and report the monitoring results to the Board of Commissioners.

5) The Board of Directors shall ensure that the risk management process of the Bank's internet banking activity is integrated into the Bank's risk management as a whole.

6) In controlling the risk management, the Board of Directors shall:

   a) establish the limit of the risks in connection with internet banking by taking into account the Bank's risk appetite;

   b) establish the delegation of authority and mechanism of reporting, including the procedures required for the

incidents impacting the Bank's financial condition and reputation;

c) take into account the risks factors specifically relating to security, integrity and availability of the internet banking services;

d) ensure that adequate due diligence and analysis of the risks have been conducted before the Bank performs the cross-border internet banking activity.

b. The Board of Directors shall approve of and restudy the main aspects of the Bank's security control procedures.

1) The Board of Directors shall continuously control the development and maintenance of the security control infrastructure that protects the internet banking system and data against any internal and external disruption.

2) The Board of Directors shall ensure that the Bank has comprehensive policies and security procedures to handle potential internal and external security disruption, in the form of both preventive measures and incident (disruption) handling. The security procedures include, among others:

a) delegation of responsibility to the Bank's officials or employees to control the Bank's security policy formulation;

b) adequate physical control to prevent unauthorized physical access to the computer room;

c) logical control procedures and adequate monitoring to prevent any internal and external unauthorized access to the internet banking application and database;

d) periodical restudy and examination of the security control steps.

3) In order to support the security control procedures in the internet banking administration, the Bank shall take into account the following matters:

a) The Bank shall formulate and maintain the security profile and establish the specific authorization privileges for the users of the internet banking system and application, such as the customers, Bank's work units/officers and service providers (outsourcing);

b) The Bank shall classify the internet banking data and systems based on sensitivity, interest and level of protection, among others by establishing the correct mechanisms, such as

inscription, control over access, and plan to recover the data to protect all the systems, servers, database and application of highly sensitive and risky internet banking;

c) storing of the highly sensitive or risky data on the Bank's computer system (desktop and laptop) shall be minimized and protected by inscription, control to access, and plan to recover the data;

d) the keys used for inscription purposes shall be kept safely so that nobody will know entirely the combination of such keys;

e) the Bank shall have adequate physical control to prevent unauthorized access to the internet banking systems, servers, database and application of internet banking;

f) the Bank shall apply various correct methods and techniques in order to reduce external threats to the internet banking system, such as:

i. the virus scanning software for all the entry points and each computer system (desktop);

ii. the software and other equipment of the security system evaluation periodically to detect infiltration;

iii. the penetration testing of the internal and external network shall be conducted periodically (at least once a year).

2. Security Control

a. The Bank shall take adequate steps to authenticate the identities and authorization of the customers who execute transactions through internet banking.

1) The Bank shall use reliable methods in the process of verifying the new customers' identities and authorization and the process of authenticating the old customers' identities and authorization.

2) The Bank shall have written policies and procedures to ensure that it is capable of authenticating the customers' identities and authorization. The Bank may use various methods for authentication, such as the personal identification number (PIN), password and digital certificate.

3) The Bank shall establish the methods of authentication based on the management's evaluation of the risks facing the internet banking activity. This risk evaluation shall also evaluate the transactional capacity in the internet banking system, such as fund transfer, bill payment, and credit withdrawal, and evaluate

the sensitivity of the value of the data stored, and the facilities for the customers to use the methods of authentication.

4) The Bank shall monitor and apply healthy internet banking practices in order to ensure that:

a) the database of authentication that provides access to the customers' accounts in internet banking is protected against disruption and damages;

b) authentication shall have been correctly authorized by the authorized party before each addition to, elimination or change of the database is made;

c) the correct facilities to control the internet banking system are available, so that unidentified third parties cannot replace the identified customers.

b. The Bank shall use the transactional authentication method in order to guarantee that the transactions cannot be denied by the customers (non-repudiation) and establish responsibility in the internet banking transactions.

The Bank shall formulate and establish the correct procedures in accordance with the significance and types of internet banking transactions, in order to ensure that:

1) the internet banking system has been designed to reduce the possibility of the execution of unintended transactions by the rightful users:

2) all the parties who execute the transactions have been authenticated;

3) the financial transaction data are protected against the possibility of changes and each change can be detected.

c. The Bank shall ensure the separation of duties in the internet banking system, database and other applications.

Establishment of the separation of duties in the internet banking system shall comply with the following matters:

1) the transactional system and process shall be designed to ensure that no employees/third parties can enter, authorise or complete any transaction;

2) available separation of duties between the party who initiates statistical data and the party who is responsible for verification of the truthfulness of the statistical data;

3) testing to ensure that application of separation of duties is not overstepped (bypassed);

4) available separation of duties between the party who develops and the party who administers the internet banking system.

d. The Bank shall ensure correct control over authorization and right to access (privileges) the internet banking system, database and other applications.

In the framework of maintaining the separation of duties, the Bank shall strictly control the authorization and use of the right to access. Failure to prepare and apply control over such authorization may enable other parties with no right to access to do things outside their authority.

The matters to be heeded are:

1) the need for authorization and right to specific access for the parties relating to the internet banking activity;

2) the internet banking system is designed by taking into account that the subsystems interact with each other in the database of authorization established by the Bank;

3) the parties relating to the internet banking activity do not represent the authority to change the authority or right to access to the internet banking authorization database;

4) any addition or change to the parties with access to the internet banking authorization database shall be authorized by the authorized party;

5) availability of correct steps to ensure that the internet banking authorization database is resistant against disruption, among others through sustainable monitoring and audit trails to document such disruption;

6) any disrupted internet banking authorization database shall not be used before it is replaced by a valid database;

7) available control to prevent any changes at the authorization level during internet banking transactions and any efforts to change the authorization shall be recorded (logged), to which the Bank management shall pay attention.

e. The Bank shall ensure that adequate procedures are available to protect the integrity of data, records/files, and information on internet banking.

Several steps that can be used by the Bank to maintain the data integrity in the internet banking system are, among others:

1) the internet banking transactions shall be resistant against any disruption in each transactional process;

2) the internet banking files shall be kept, accessed and modified in such a way as to be resistant against any disruption;

3) the internet banking transactions and recording process shall be designed in such a way as to prevent illegal changes;

4) adequate monitoring and testing procedures are available so that any changes to the internet banking system will not reduce the data reliability;

5) any changes to the internet banking transactions or recording shall be detectable through the transactional processing, monitoring and recording maintenance.

f. The Bank shall ensure the availability of obvious audit trails for all the internet banking transactions.

1) In order to ensure the availability of obvious audit trails, the types of the internet banking transactions that shall be heeded are, among others:

a) opening, modification or closing of a customer's account;

b) any transactions with financial impacts;

c) any authorization that allows customers to exceed the established limits;

d) any provision, modification and revocation of rights and authority to access the system.

2) The matters that shall be heeded in order to ensure available obvious audit trails are, among others:

a) the records/logs shall be kept for all the internet banking transactions in order to provide obvious audit trails and help in dispute settlement;

b) the audit trails and other logs, such as the audit log tools for detecting infiltration, shall be reviewed/ evaluated periodically;

c) the internet banking system shall be designed in order to obtain forensic evidence and prevent disruption and gathering of incorrect evidence;

d) if the processing system and the audit trails are the responsibility of the third party, the Bank shall have access to the audit trails kept by the third party and such audit trails shall be in accordance with the standard established by the Bank.

g. the Bank shall take steps to protect the confidentiality of essential information on internet banking. The steps shall be in accordance with the sensitivity of the information issued and/or kept in the database.

In order to maintain confidentiality of essential information on internet banking, the Bank shall ensure that:

1) all the Bank's confidential files and data can only be accessed by the authorized parties and the authentication has been proven;

2) all the Bank's confidential data shall be maintained safely against the possibility of being known or modified by transmission through public, personal or internal networks;

3) the Bank shall have the standard and control over the use and protection of the data if the third party/outsourcing has access to such data;

4) all the access to the limited data shall be kept (logged) and correct steps shall be taken in order to ensure that the data are resistant to disruption.

3. Legal and Reputation Risks Management

a. The Bank shall ensure that its website provides the information that enables prospect customers to obtain correct information on the Bank's identity and legal status before making any transaction through the internet banking. The information provided in the Bank's website includes, among others:

1) the Bank's name and domicile;

2) the identity of the Bank's control authority;

3) the procedures for the customers to access the customer service unit if there are any problems, claims, misuses of the accounts, etc.;

4) the procedures for the customers to access the customer complaint program;

5) the procedures for the customers to obtain information on deposit security and protection of other customers;

6) other relevant information.

b. The Bank shall take the steps to ensure that the regulations on customer confidentiality are applied as those applicable in the country where the Bank is domiciled to provide the internet banking products and services.

1) Misuse of disclosure of customer data confidentiality can cause the Bank to be exposed to the legal and reputation risks. Therefore, the Bank shall take actions to ensure that:

a) the policy and standard of customer confidentiality are in accordance with the prevailing legislation on customer confidentiality/Bank's secrets;

b) the customers are provided with the understanding of the Bank's customer confidentiality policy and other relevant confidentiality issues in connection with the use of the internet banking products and services;

c) the customer data are not used for other purposes than those generally allowed or outside the authority provided by the customers;

d) the standard use of the customer data shall be fulfilled if the third party (outsourcing) has access to the customer data.

2) In order to support the application of the information confidentiality of the customers who execute transactions through internet banking, the Bank shall heed the following matters:

a) use of inscription techniques, special procedures and other security control to ensure the internet banking customer data confidentiality;

b) development of adequate procedures and control to evaluate the internet banking customer security infrastructure and procedures periodically;

c) certainty that the third party (outsourcing) used by the Bank has the confidential policy consistent with that of the Bank;

d) taking of the steps to inform the internet banking customers on the customer information confidentiality policy, including:

(1) providing brief and clear information for the customers on the Bank's confidentiality policy, among others through the Bank's website;

(2) providing instructions for the customers on the importance of keeping the passwords, personal identification numbers (PINs) and other banking and/or personal data;

(3) providing information for the customers on their personal computer security techniques, including the benefit in using the software to control viruses, control of the physical access and the personal firewall to connect the Internet.

c. The Bank shall have effective emergency planning procedures and business sustainability to ensure the availability of the internet banking system and services.

1) The Bank shall be able to provide the internet banking services through the in-house system and application and outsourcing for the customers consistently and timely.

2) In order to guarantee business sustainability of the internet banking services, the Bank shall ensure:

a) the capacity of the available internet banking system and the increased volume of transactions in the future analyzed on the basis of external development and projection of the level of receipt of the internet banking products and services by the customers;

b) the periodical examination and restudy of the internet banking transaction processing capacity;

c) the periodical examination of the business sustainability and emergency planning for the processing and system of delivering the internet banking services.

3) Several steps that the Bank shall consider in the framework of the emergency planning application, business sustainability and improved quality of the internet banking capacity are, among others:

a) the Bank shall identify and review all the internet banking applications and services, including those provided by the service provider/third party;

b) the Bank shall evaluate the risks on each internet banking service and application, including the implications that may arise, such as the risks of credits, markets, liquidity, legal, operational and reputation, that may disrupt the Bank's business activities;

c) The Bank shall establish the performance criteria for each internet banking service and application and monitor their implementation compared to such performance criteria;

d) the Bank shall take correct steps to ensure that the internet banking system is capable of coping with big and small transaction volumes, and that the performance and capacity of the system are consistent with its plan to develop internet banking in the future;

e) the Bank shall develop several alternative procedures if the internet banking system is going to reach certain capacity limits;

f) the Bank shall have the internet banking system recovery procedures to maintain business sustainability in order to reduce dependency on the service provider/third party and other external parties;

g) the internet banking emergency plan shall include the procedures to recover or replace the internet banking processing capacity, reconstruct the supporting transactional information, and recover the existence of the internet banking system and applications if the business activities are disrupted.

d. The Bank shall develop an adequate handling plan to manage, cope with and minimize the problems arising out of unpredicted occurrences

(internal and external) that may hamper the provision of the internet banking system and services.

1) The Bank shall develop communication strategies that can ensure business sustainability, control the reputation risks, and restrict its obligations in connection with disrupted internet banking services, including those originating from the system and operation handled by the third party.

2) In order to ensure effective handling of unpredicted occurrences, the Bank shall develop:

    a) the occurrence handling plan to recover the internet banking system and services in various scenarios;

    b) the mechanisms to identify any occurrence, evaluate its materiality, and control the reputation risks relating to the disruption in providing the internet banking services;

    c) the strategy of communication with external parties and the media in order to cope with the problems that may arise as the consequence of security failure, disrupted online system and internet banking system;

    d) an occurrence handling team with the authority to act in case of emergency and with the competency to analyze the

detection system and evaluate the results/outputs of the detection system;

e) clear instructional mechanisms to ensure that the actions taken are appropriate corrective actions;

f) the procedures of delivering information quickly and correctly to the Bank customers, counterparty, and the media on the causes of the internet banking disruption and its handling development;

g) the procedures of gathering and keeping the forensic evidence to facilitate the study on the occurrences relating to the internet banking activity and for helping in the process of legal claims against the external parties who disrupt the internet banking.

e. If the internet banking system is applied by the third party (outsourcing), the Bank shall establish and apply comprehensive and sustainable control procedures and due diligence to manage the relationship of the Bank and the third party.

In managing the relationship, the Bank shall ensure that:

1) it fully understands the risks relating to the outsourcing agreement or cooperation on the provision of the internet banking system and application;

a) the Bank shall identify the strategic objectives and the profits and losses relating to the use of outsourcing in internet banking;

b) the decision to carry out outsourcing in internet banking shall be consistent with the Bank's business strategies by taking into account the characteristics of the risks adhering to the use of outsourcing;

c) in accordance with the operating structure, the Bank's work units shall understand the work procedures of the service providers who apply the internet banking strategy.

2) implementation of adequate due diligence on the competency and financial condition of the third party who provides services before entering into any internet banking service contract:

a) the Bank shall consider the process development and establish the criteria/ requirements for the selection of several service providers;

b) the Bank shall conduct due diligence, including risk analysis, financial condition, reputation, policy, risk management control and capacity of the service providers, to fulfil their obligations;

c) the Bank shall monitor and review periodically the capacity of the service providers to render their services and fulfil their obligation of risk management application during the contract period;

d) the Bank shall ensure availability of adequate human resources and be committed to control the outsourcing that administers internet banking;

e) the Bank shall establish obvious responsibilities of the work units or officers in respect of control over the outsourcing management;

f) the Bank shall establish the correct exit strategy to manage the outsourcing risks if the contract with the outsourcing party is to be terminated.

3) clarity of the scope of each party's responsibility in contractual agreements with the third party in connection with:

a) the contractual obligations of the appointed parties and the responsibility to make decisions, including the subcontract services;

b) the responsibility to provide information for and receive information from the service providers, namely that the information from the service providers shall be timely and

comprehensive, so as to enable the Bank to evaluate the level and risks of the internet banking services;

c) the regulations that specifically establish insurance coverage, ownership of the stored data or database of the service providers and the Bank's right to recover the data that have exceeded a certain time limit and termination of contract;

d) the service providers' performance expectations in both normal and emergency situations;

e) availability of adequate security arrangement, for instance, through the audit clauses ensuring that the service providers comply with the Bank's policies;

f) clauses that arrange the Bank's right to make timely correction and intervention if the performance and service providers' are not in accordance with the contract (below the agreed standard);

g) establishment of certain state legislation on customer confidentiality and protection, particularly for the arrangement of cross-border outsourcing;

h) availability of the clauses on the Bank's right to conduct independent reviews and/or audits of the security system,

internal control, business sustainability and emergency planning.

4) operation and provision of the internet banking system by the third party have been in accordance with the policies on risk management, security and confidentiality applicable in the Bank.

5) audits by external and internal independent auditors shall be periodically conducted on the internet banking operation by the third party with the same audit frequency and coverage if internet banking is administered in-house.

6) availability of adequate emergency planning for the internet banking activity operated by the third party by means of, among others:

   a) the Bank shall develop and test periodically the emergency planning of the internet banking services and system operated by the third party;

   b) the emergency planning shall contain the Bank's handling steps in the worst case scenario, so that the internet banking business can continue despite the disruption that may affect the operations conducted by the third party;

   c) the Bank shall have special teams and officers responsible for managing the recovery and for evaluating the financial

impacts caused by any disruption to the internet banking system operated by the third party.

---------- *00* ----------